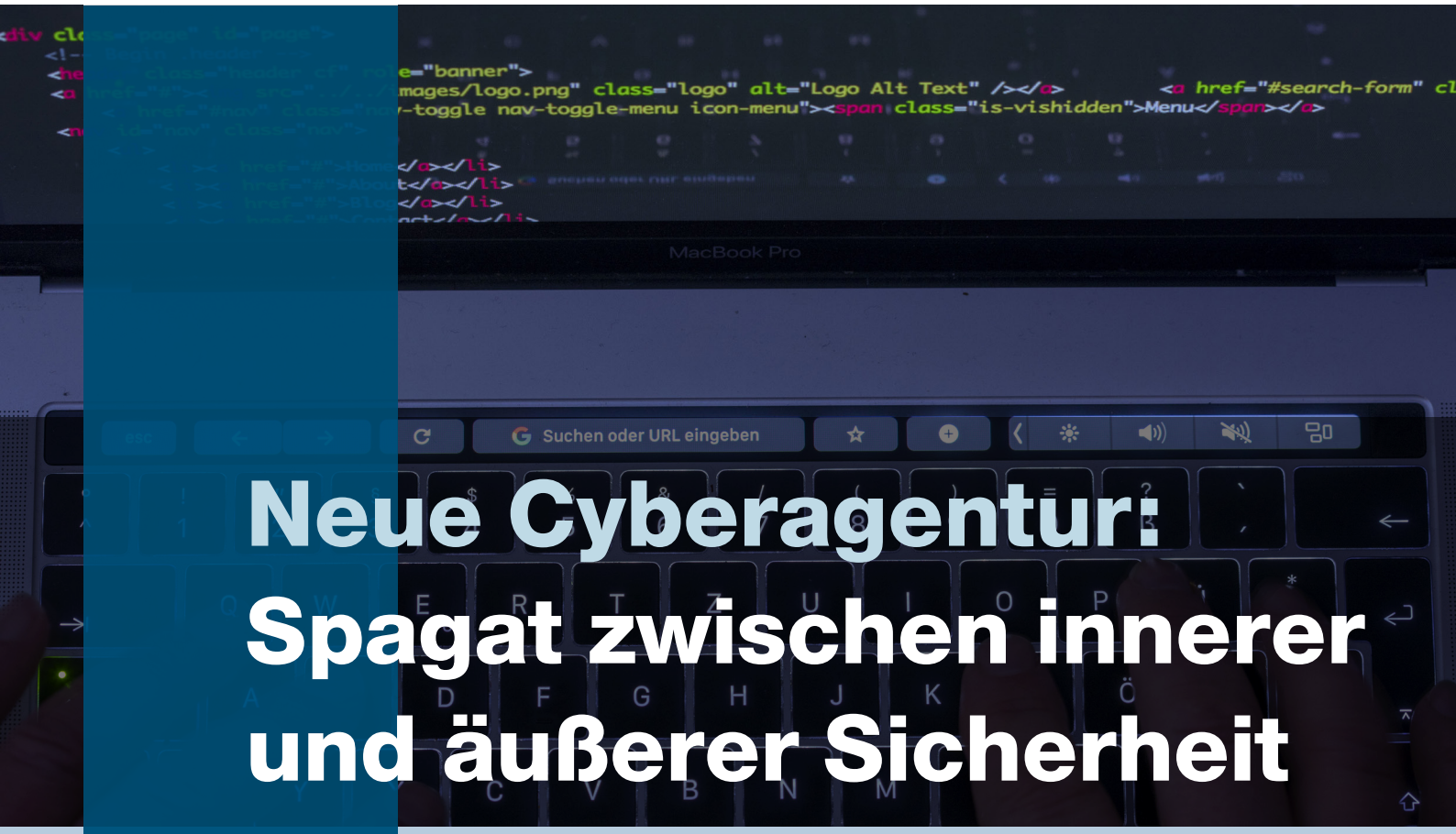
Neue Cyberagentur: Spagat zwischen innerer und äußerer Sicherheit

Reinhold, Thomas

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Empfohlene Zitierung / Suggested Citation:
Reinhold, T. (2019). *Neue Cyberagentur: Spagat zwischen innerer und äußerer Sicherheit.* (IFSH Policy Brief, 04/19). Hamburg: Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). https://doi.org/10.25592/ifsh-policy-brief-0419

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



Neue Cyberagentur: Spagat zwischen innerer und äußerer Sicherheit

Die Bekämpfung von Internet-Kriminalität und die Abwehr von Spionage sowie militärischen Angriffen aus dem Netz erfordern technisches Know-how, rechtliche Befugnisse und eine gezielte Zusammenarbeit der staatlichen Organe. Die neu geschaffene Agentur für Innovation in der Cybersicherheit soll hier künftig eine zentrale Rolle spielen, allerdings wirft die neue Behörde auch einige Fragen auf:

- Die Grenzen von innerer und äußerer Sicherheit verschwimmen, weil die Behörde ein Gemeinschaftsprojekt verschiedener Ministerien ist.
- Die rechtliche Konstruktion der Behörde erschwert ihre parlamentarische Kontrolle.
- Schon jetzt existieren zahlreiche Initiativen zur Sicherheit im Cyberspace. Eine weitere staatliche Behörde macht es noch schwieriger, die Aufgaben der einzelnen Einrichtungen zu koordinieren.
- Die Agentur fördert vor allem militärische und nachrichtendienstliche Projekte – für die zivile IT-Sicherheit wird weiterhin zu wenig getan.

04|19

THOMAS REINHOLD | 2019

Anfang des Jahres stellten unbekannte Hacker private Daten von Spitzenpolitikern ins Netz: Telefonnummern, private Fotos, Kontodaten. Nicht der erste digitale Angriff auf den Bundestag, aber einer der spektakulärsten. Schon in ihrem Koalitionsvertrag von 2018 hatte die Bundesregierung die Gründung einer Agentur für Innovation in der Cybersicherheit beschlossen – ganz nach dem Vorbild der amerikanischen Defense Advanced Research Projects Agency (DARPA). Die Aufgabe der neuen Agentur: Sie soll für die Nachrichtendienste und die Bundeswehr Schlüsseltechnologien im Cyberspace entwickeln und fördern.

An der Gründung der Agentur waren sowohl das Bundesverteidigungs- als auch das Bundesinnenministerium beteiligt. Bis 2020 investiert die Bundesregierung insgesamt 200 Millionen Euro in ihren Aufbau. Das Geld wird zum größten Teil direkt in Forschungs- und Innovationsvorhaben fließen. Denn die rund 100 Mitarbeiterinnen und Mitarbeiter der Agentur forschen nicht selbst. Vielmehr soll die neue Behörde, die ihren Sitz in der Nähe des Flughafens Halle/Leipzig haben wird, wissenschaftliche Projekte finanzieren und Deutschland damit einen Spitzenplatz in der Sicherheitsforschung sichern. Die Ergebnisse der Forschung sollen vor allem den Nachrichtendiensten und dem Militär dienen und Deutschlands innere und äußere Sicherheit stärken. Eine zivile Nutzung der Projekte ist nicht vorgesehen.

„OFFENSIVE FÄHIGKEITEN ZU FÖRDERN, WÜRDE ZUR WEITEREN MILITARISIERUNG DES CYBERSPACE BEITRAGEN.“

UNKLARE ABGRENZUNG GEGENÜBER WEITEREN EINRICHTUNGEN

Neben dieser neuen Agentur starteten die beiden Ministerien in den vergangenen Monaten bereits weitere Initiativen. Dazu zählt der *Cyber Innovation Hub* des Bundesverteidigungsministeriums, der Startup-Unternehmen unterstützt, die militärisch anwendbare Ideen zur Cybersicherheit entwickeln. Darüber hinaus wurde die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)* des Bundesinnenministeriums gegründet, ein technischer Dienstleister für Behörden der inneren Sicherheit. Explizite Kooperationen der Einrichtungen sind nicht vorgesehen, ihre Forschungsbereiche sollen sich nicht überschneiden. Weil die beiden jüngst gegründeten Einrichtungen bereits ähnliche Aufgaben wahrnehmen, könnte man vermuten, dass die neue Agentur dafür zuständig sein wird, wie Nachrichtendienste und Bundeswehr fremde IT-Systeme ausspähen oder stören können. Eine solche politische Priorisierung, offensive Fähigkeiten zu fördern, würde zur weiteren Militarisierung des Cyberspace beitragen.

GRENZEN ZWISCHEN INNERER UND ÄUSSERER SICHERHEIT VERSCHWIMMEN

Kriminalität, Vandalismus und Spionage im Netz: All das sicherheitspolitisch zu bewerten ist ein komplexes Unterfangen, eine effiziente und spannungsfreie Zusammenarbeit ist für alle beteiligten Ministerien und Behörden eine Herausforderung. 2016 verab-

schiedete die Bundesregierung die sogenannte *Cyber-Sicherheitsstrategie*. Damals wurde das Nationale *Cyber-Abwehrzentrum* als zentrale Koordinationsstelle geschaffen, das Lagebilder erstellt und im Krisenfall die Arbeit der staatlichen Stellen koordiniert. Alle beteiligten Behörden orientieren sich an den rechtlichen Rahmenbedingungen. Besonders sensible Bereiche, etwa mit Geheimhaltungsstufe oder erweiterten Eingriffsbefugnissen, unterliegen demokratischen Kontrollmöglichkeiten, die Kooperation zwischen den Einrichtungen ist klar definiert und begrenzt. Bei der neu gegründeten Agentur, die dazu noch als GmbH etabliert werden soll, fehlt dies alles. Es stellt sich die grundsätzliche Frage, ob die engere Zusammenarbeit der Institutionen mit gegenseitig abgestimmten Forschungsvorhaben und Nutzungsinteressen demokratisch legitimierbar und kontrollierbar ist.

„DIE FRAGE IST, OB EINE ENGE ZUSAMMENARBEIT DER INSTITUTIONEN DEMOKRATISCH LEGITIMIERBAR UND KONTROLLIERBAR IST.“

PROBLEMATISCHE KOOPERATION DER GEHEIMDIENSTE

Eine solche explizite Kooperation mit dem Ziel der gemeinsamen Technologieförderung ist in Deutschland bislang einmalig. Fraglich ist, warum ein solcher Schritt aus Sicht der Ministerien überhaupt notwendig ist. Außerdem bleibt unklar, wo es gemeinsame Aufgaben und technologische Bedürfnisse gibt, die nur in dieser Form abgedeckt werden. Schließlich wäre es auch möglich, zivile Maßnahmen zu fördern, etwa durch das Bundesforschungs- oder Wirtschaftsministerium oder die Wirtschaft selbst. Doch nicht nur die Transparenz- und Kontrollmöglichkeiten sind diffus. Die geförderten Projekte werden durch ihren militärischen Einsatzbereich zwangsläufig einer strengen Kontrolle durch Rüstungs- und Exportkontrollkontrollabkommen unterliegen. Dies könnte für die beteiligten Forschungs- und Wirtschaftsunternehmen bei der Vermarktung ihrer Ideen von großem Nachteil sein.

KLARE AUFGABENVERTEILUNG UND FÖRDERUNG ZIVILER IT-SICHERHEIT HABEN HÖCHSTE PRIORITÄT

Angriffe aus dem Internet sind eine große Herausforderung für die nationale Sicherheit. Deshalb sollte der Fokus darauf liegen, zivile defensive IT-Sicherheitstechnologien zu fördern, die Behörden, Unternehmen und Bürgern gleichermaßen bereitstehen. Für die Cybersicherheit sollen und müssen alle zuständigen Behörden und Stellen zusammenarbeiten. Diese institutionelle Kooperation sollte aber besser aufeinander abgestimmt und fachlich abgegrenzt sein als dies bislang der Fall ist. Nur so können die bestehenden gesetzlichen Trennungen zwischen Behörden und Diensten gewahrt werden. Schnelle Entscheidungswege und Reaktionsmechanismen sind entscheidend, damit im Krisenfall notwendige Kapazitäten bereitstehen und organisationsübergreifend effektiv eingesetzt werden können. Ein solcher Weg wurde mit dem aufgewerteten *Nationalen Cyber-Abwehrzentrum* beschritten, das eine Plattform für alle Beteiligten bietet und als zentraler Ansprechpartner für internationale Kooperationen bereitsteht. In ähnlicher Weise sollte das Bundesamt für Sicherheit und Informationstechnik aufgewertet werden. Es sollte weitere Zuständigkeiten bekommen, um Vorfälle einordnen und technisches Know-how zum Schutz von IT-Systemen bereitstellen zu können. Eine zu unklare Abgrenzung von Zuständigkeiten und eine zu unscharfe Definition, was die neue Agentur überhaupt rechtlich darf, wird vor allem zu einem führen: Die fachliche und organisatorische Situation bei Cyberangriffen wird noch unübersichtlicher als sie es jetzt schon ist.

ÜBER DEN AUTOR

Thomas Reinhold ist Non-Resident Fellow am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg.

ÜBER DAS INSTITUT

Das Institut für Friedensforschung und Sicherheitspolitik (IFSH) erforscht die Bedingungen von Frieden und Sicherheit in Deutschland, Europa und darüber hinaus. Das IFSH forscht eigenständig und unabhängig. Es wird von der Freien und Hansestadt Hamburg finanziert.

Gefördert von:

Hamburg | Behörde für Wissenschaft, Forschung und Gleichstellung

IFSH – **Institut für Friedensforschung und Sicherheitspolitik** an der Universität Hamburg
Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077-0 ifsh@ifsh.de www.ifsh.de